

# Valid Dumps ISO-IEC-27001-Foundation Ppt & Official ISO-IEC-27001-Foundation Study Guide



P.S. Free & New ISO-IEC-27001-Foundation dumps are available on Google Drive shared by Lead2Passed: [https://drive.google.com/open?id=15FMe\\_6b9HmuN-DQMHCck006IBdQWSPQF](https://drive.google.com/open?id=15FMe_6b9HmuN-DQMHCck006IBdQWSPQF)

If you are planning to pass the ISO-IEC-27001-Foundation exam, you can choose our ISO-IEC-27001-Foundation practice materials as your learning material since our products are known as the most valid exam engine in the world, which will definitely be beneficial to your preparation for exams. There are many impressive advantages of our ISO-IEC-27001-Foundation Study Guide. And our ISO-IEC-27001-Foundation actual exam will be definitely conducive to realizing the dream of obtaining the certificate.

Your eligibility of getting a high standard of career situation will be improved if you can pass the exam, and our ISO-IEC-27001-Foundation study guide are your most reliable ways to get it. You can feel assertive about your exam with our 100 guaranteed professional ISO-IEC-27001-Foundation Practice Engine for you can see the comments on the websites, our high-quality of our ISO-IEC-27001-Foundation learning materials are proved to be the most effective exam tool among the candidates.

>> Valid Dumps ISO-IEC-27001-Foundation Ppt <<

## Official ISO-IEC-27001-Foundation Study Guide, ISO-IEC-27001-Foundation Guide

Getting the APMG-International ISO-IEC-27001-Foundation certification exam is necessary in order to get a job in your desired tech company. Success in the ISO/IEC 27001 (2022) Foundation Exam (ISO-IEC-27001-Foundation) certification exam gives you an edge over the others because you will have certified skills. The APMG-International ISO-IEC-27001-Foundation certification exam badge will make a good impression on the interviewer. Most of the people planning to attempt the ISO-IEC-27001-Foundation Exam are confused that how will they prepare and pass ISO-IEC-27001-Foundation exam with good grades. Many don't find real ISO-IEC-27001-Foundation exam questions and face loss of money and time.

### APMG-International ISO-IEC-27001-Foundation Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none"> <li>Security Breaches: Security breaches occur when unauthorized access or violations of security protocols are detected or imminent, potentially compromising data or system integrity.</li> </ul>
Topic 2	<ul style="list-style-type: none"> <li>Framework Design: Framework design is the process of developing a reusable structural foundation that supports and guides the creation and organization of software systems.</li> </ul>

Topic 3	<ul style="list-style-type: none"> <li>• Risk Management: Risk management is the systematic process of identifying, evaluating, and implementing strategies to reduce or control the impact of potential uncertainties on organizational goals.</li> </ul>
Topic 4	<ul style="list-style-type: none"> <li>• Self Confidence: Self-confidence is the belief in one's abilities, competence, and value, reflecting a sense of assurance and inner strength.</li> </ul>
Topic 5	<ul style="list-style-type: none"> <li>• Compliance: Regulatory compliance refers to an organization's commitment to understanding and adhering to applicable laws, policies, and regulations to operate within established legal and ethical standards.</li> </ul>
Topic 6	<ul style="list-style-type: none"> <li>• Continuous Improvement Process (CI, CIP): A continuous or continual improvement process (CIP or CI) involves ongoing, systematic efforts to enhance products, services, or operational processes to achieve higher efficiency and effectiveness over time.</li> </ul>

## APMG-International ISO/IEC 27001 (2022) Foundation Exam Sample Questions (Q21-Q26):

### NEW QUESTION # 21

Which of the following is required to be considered when selecting appropriate information security risk treatment options?

- A. Criteria for accepting identified risks
- B. Only risk controls in ISO/IEC 27002
- C. Only risk controls in Annex A of ISO/IEC 27001
- D. Criteria for performing risk assessments

**Answer: A**

Explanation:

Clause 6.1.3 (c) requires organizations to:

"compare the controls determined in 6.1.3 b) with those in Annex A and verify that no necessary control has been omitted; and prepare a Statement of Applicability." It also requires organizations to select risk treatment options considering "the organization's risk acceptance criteria." This shows that risk acceptance criteria are a fundamental factor when selecting risk treatment options.

Options C and D are incorrect because Annex A and ISO/IEC 27002 are reference sets, not the sole sources of controls - organizations can design their own. Criteria for performing risk assessments (B) are part of 6.1.2 (risk assessment process), not risk treatment.

Thus, the correct requirement is A: Criteria for accepting identified risks.

### NEW QUESTION # 22

Who determines the number of days required for a certification audit?

- A. Both the management representative and the external auditor together
- B. The lead internal auditor from the organization to be audited
- C. The external auditor from the Certification Body who will undertake the audit
- D. The management representative from the organization to be audited

**Answer: C**

Explanation:

Certification audits are carried out by Certification Bodies (CBs), not the organization itself. ISO/IEC 27001 requires external certification audits to be independent, impartial, and objective. According to ISO/IEC 27006 (Requirements for bodies providing audit and certification of ISMS), the Certification Body determines the audit duration and number of audit days based on factors such as organizational size, complexity, scope, and risk environment. This ensures consistency across organizations and prevents manipulation by the auditee. ISO/IEC 27001 Clause 9.2 and 9.3 address internal audit and management review, but the determination of certification audit days is outside the organization's control; it rests solely with the accredited Certification Body auditors. Thus, answer: C is correct, as the CB's external auditor formally calculates and assigns the audit time.

### NEW QUESTION # 23

Which statement about the conduct of audits is true?

- A. During Stage 1 of a certification audit, evidence is collected by observing activities
- **B. One of the focus areas for a surveillance audit is the output from internal audits and management reviews**
- C. Third party audits are conducted by a customer of the organization
- D. The certificate issued after a successful re-certification audit in typical schemes lasts for one year

**Answer: B**

Explanation:

Clause 9.2 (Internal Audit) and Clause 9.3 (Management Review) highlight that audit outputs and management reviews are key inputs for evaluating ISMS performance. Surveillance audits, conducted by Certification Bodies, check ongoing compliance and effectiveness. ISO certification schemes (per ISO/IEC

17021) require surveillance audits to verify whether corrective actions and continuous improvements are being made. A critical focus area is the results of internal audits and management reviews, ensuring that the organization maintains its ISMS between certification cycles.

Option A is incorrect - third-party audits are performed by independent Certification Bodies, not customers.

Option B is incorrect - certificates are typically valid for three years with annual surveillance. Option D is incorrect - Stage 1 is primarily a documentation and readiness review, not evidence observation.

Therefore, the verified correct answer is C.

#### NEW QUESTION # 24

In which clause would the requirements for internal audit be found?

- A. Planning
- B. Improvement
- C. Operation
- **D. Performance Evaluation**

**Answer: D**

Explanation:

The requirements for internal audit are explicitly placed in Clause 9.2 (Performance Evaluation) of ISO/IEC 27001:2022. The standard requires:

\* "The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system... conforms to the organization's own requirements... and to the requirements of this document." (9.2.1)

\* "The organization shall plan, establish, implement and maintain an audit programme(s)..." (9.2.2) This clause clearly falls under Performance Evaluation (Clause 9), not Planning (Clause 6), Operation (Clause 8), or Improvement (Clause 10). Therefore, the correct answer is C.

#### NEW QUESTION # 25

Which statement describes the control for the Compliance with policies, rules and standards for information security within Annex A of ISO/IEC 27001?

- A. Maintain contact with legal authorities
- **B. Regular review of compliance**
- C. Return assets to their legal owners
- D. Regular review of contractual compliance

**Answer: B**

Explanation:

Comprehensive and Detailed Explanation From Exact Extract ISO/IEC 27002:2022 standards:

Annex A.5.36 (Compliance with policies, rules and standards for information security) requires:

"Compliance with the organization's information security policies, rules and standards for information security should be regularly reviewed." This directly matches option A. Option B refers to contractual compliance, which is part of supplier management controls (Annex A.5.19). Option C relates to Annex A.5.7 (Contact with authorities). Option D refers to asset return controls (Annex A.5.9).

Thus, the correct answer is A.

